WHAT IS CLAIMED

1. A method for controllably encrypting data to be transmitted over a communication path between a data source and a data recipient, comprising the steps of:

(a) providing a plurality of respectively different data encryption operators, and of which may be used, but none of which is necessarily required to encrypt said data into an unintelligible form for transmission over said communication path;

(b) passing said data to be transported over said communication path through a first of said respectively different encryption operators to thereby produce a first encrypted data stream; and

(c) passing said first encrypted data stream through a second selected one of said respectively different data encryption operators to thereby produce a compound encrypted output data stream that is an encryption of said first encrypted data stream.

2. A method according to claim 1, further including the steps of:

(d) transporting said compound encrypted output data stream over said communication path to said data recipient; and

(e) passing said output data stream through a sequence of second and first decryption operators that respectively decrypt data that has been encrypted by said second and first encryption operators, so as to recover said data.

3. A method according to claim 1, wherein step (a) comprises storing said plurality of respectively different data encryption operators in an encryption operator database, and wherein step (b) comprises retrieving said first encryption operator from said database and passing said data to be transported over said communication path through said retrieved first encryption operator to thereby produce a first encrypted data stream, and step (c) comprises retrieving said second encryption operator from said database and passing said first encrypted data stream through said second encryption operator to thereby produce said compound encrypted output data stream.

4. A method according to claim 1, further including the steps of:

(d) transporting said compound encrypted output data stream over said communication path to said data recipient; and

(e) passing said compound output data stream through a sequence of second and first decryption operators that respectively decrypt data that has been encrypted by said second and first encryption operators, so as to recover said data.

5. A method according to claim 4, wherein step (e) comprises storing a plurality of respectively different data decryption operators in a decryption operator database, retrieving from said decryption operator database second and first decryption operators that respectively decrypt data that has been encrypted by said second and first encryption operators, and passing said compound output data stream through a sequence of said second and first decryption operators so as to successively decrypt said compound output data stream and thereby recover said data.

6. A method for controllably encrypting data to be transmitted over a communication path between a data source and a data recipient, comprising the steps of:

(a) providing a plurality of respectively different data encryption operators;

(b) sequentially passing data to be transported over said communication path through multiple ones of said respectively different data encryption operators to thereby produce a compound-encrypted data stream.

7. A method according to claim 6, further including the steps of:

(c) transporting said compound-encrypted data stream over said communication path to said data recipient; and

(d) passing said compound-encrypted data stream through a sequence of multiple decryption operators that sequentially decrypt said compound-encrypted data so as to recover said data.

8. A method for controllably encrypting data to be transmitted over a communication path between a data source and a data recipient, comprising the steps of:

(a) storing a plurality of respectively different data encryption operators in a data encryption operator database;

(b) retrieving from said database and assembling selected ones of said respectively different data encryption operators into a sequence of data encryption operators, wherein immediately successive ones of said data encryption operations of said sequence are different from one another; and

(c) passing data to be transported over said communication path through said sequence of data encryption operators generated in step (b), so as to produce a compound-encrypted data stream.

9. A method according to claim 8, further including the steps of:

(d) transporting said compound-encrypted data stream over said communication path to said data recipient;

(e) retrieving from a decryption operator database in which a plurality of respectively different data decryption operators are stored, respective decryption operators that respectively decrypt data that has been encrypted by said selected encryption operators;

(f) passing said compound-encrypted output data stream through a sequence of decryption operators retrieved in step (e), successively decrypting said compound-encrypted data stream and thereby recover said data.

10. A method for controllably encrypting data to be transmitted over a communication path between a data source and a data recipient, comprising the steps of:

(a) providing a plurality of respectively different data encryption operators;

(b) generating a sequence of data encryption operators comprised of plural ones of said respectively different data encryption operators provided in step (a); and

(c) passing data to be transported over said communication path through said sequence of data encryption operators generated in step (b), so as to produce a compound-encrypted output data stream.

11. A method according to claim 10, further including the steps of:

(d) transporting said compound-encrypted output data stream over said communication path to said data recipient; and

(e) passing said compound-encrypted output data stream through a sequence of decryption operators that respectively decrypt data that has been encrypted by said data encryption operators, so as to recover said data.

12. A method for controllably encrypting data to be transmitted over a communication path between a data source and a data recipient, comprising the steps of:

(a) storing a plurality of respectively different data encryption operators;

(b) generating a sequence of access codes, each of which is associated with a respective one of said data encryption operators stored in step (a), with immediately successive ones of said access codes of said sequence being different from one another;

(c) accessing selected ones of said respectively different data encryption operators stored in step (a) in accordance with said sequence of access codes generated in step (b), so as to produce a sequence of data encryption operators, in which immediately successive ones of said data encryption operators are different from one another; and

(d) passing data to be transported over said communication path through said sequence of data encryption operators produced in step (c) to produce a compound-encrypted data stream.

13. A method according to claim 12, further including the steps of:

(e) transporting said compound-encrypted output data stream over said communication path to said data recipient; and

(f) passing said compound-encrypted output data stream through a sequence of decryption operators that respectively decrypt data that has been encrypted by said data encryption operators, so as to recover said data.

14. A system for controllably encrypting data to be transmitted over a communication path between a data source site and a data recipient site, comprising:

at said data source site,

a data encryption operator database which stores a plurality of respectively different data encryption operators;

an address code generator which generates a sequence of access codes, each of which is associated with a respective one of said data encryption operators stored in said data encryption database, such that immediately successive ones of said access codes of said sequence differ from one another, so as to access from said data encryption operator database a sequence of stored data encryption operators, such that immediately successive ones of retrieved data encryption operators are different from one another; and

a signal processor which is operative to apply data to be transported over said communication path through said sequence of data encryption operators accessed from said encryption operator database to produce a compound-encrypted data stream for transport over said communication path.

15. A system according to claim 14, further including, at said data recipient site,

a data decryption operator database which stores a plurality of respectively different data decryption operators;

an address code generator which generates a sequence of access codes, each of which is associated with a respective one of said data decryption operators stored in said data decryption database, and is operative to cause a sequence of data decryption operators to be accessed from said data decryption database in accordance with the reverse order of said sequence of data encryption operators that produced said compound-encrypted data stream; and

a signal processor which is operative to apply said compound-encrypted data stream that has been transported over said communication path to said data recipient site through said sequence of data encryption operators accessed from said encryption operator database to recover said data.